EDItran Proxy 4.1

CICS-IMS (Windows-UNIX)

Manual de instalación y usuario.

Indra.
Enero - *2005.*
EPR41USIA.doc.

Indra.

La información aquí contenida puede ser objeto de cambios sin previo aviso. Las distintas versiones del producto pueden dar lugar a cambios, adiciones o supresiones de información en este manual.
La correspondencia acerca de este manual debe realizarse en la hoja de comentarios aquí incluida y debe ser dirigida a Indra, Producto EDItran, Avda. de Bruselas 35 (Edificio VIO-1), 28108 - Arroyo de la Vega - Alcobendas, Madrid.

Comentarios de usuario sobre esta documentación.
Exprese, y háganos llegar, su opinión y comentarios acerca de la documentación entregada y así podremos corregirla en las posteriores versiones de este documento.

Indra.

Producto : EDItran Proxy 4.1 CICS-IMS

Manual de instalación y usuario.

Referencia: **EPR41USIA.doc**

Avda. de Bruselas 35 - Arroyo de la Vega - Alcobendas.

28108 MADRID.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Empresa :
_____

Departamento: _____

Contacto :
_____

Dirección :
_____

1. INTRODUCCION Y REQUERIMIENTOS. 1-1

2. DEFINICIONES Y CAMBIOS (OS/390 ï Z/OS). 2-1

2.1. VERSIÓN CICS 2-1
2.1.1. DEFINICIONES. 2-1
2.1.2. CAMBIOS EN EDItran/P. 2-1
2.1.3. BACKUP. 2-4
2.1.4. Mensajes de error xô20ôy liberación xô13ô. 2-4
2.2. VERSIÓN IMS 2-5

3. CARACTERÍSTICAS PRINCIPALES 3-1

3.1. MULTIPLATAFORMA 3-1
3.2. OPTIMIZACIÓN (MULTITHREADING) 3-1
3.3. TIMEOUT 3-1
3.4. BOMBING 3-1
3.5. SEGURIDAD 3-1
3.6. VALIDACIÓN DE PROTOCOLO EDITRAN 3-1
3.7. GENERACIÓN DE SYSLOG 3-2

4. EDITRAN/PROXY EN UNIX Y WINDOWS 4-1

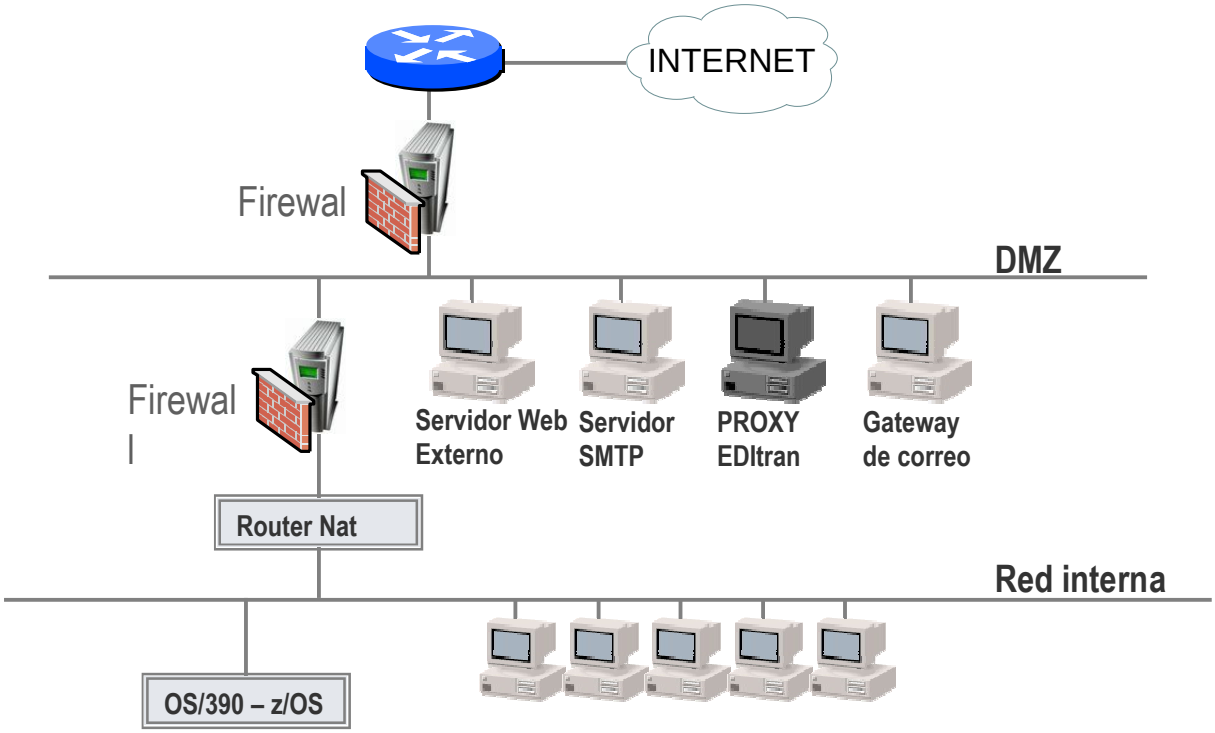
4.1. INSTALACIÓN DE EDITRAN/PROXY EN UNIX 4-1
4.2. INSTALACIÓN DE EDITRAN/PROXY EN WINDOWS 4-1
4.3. CONFIGURACIÓN DE EDITRAN/PROXY WINDOWS 4-1
4.4. ARRANQUE Y PARADA WINDOWS 4-1
4.5. NOTIFICACIONES SYSLOG 4-1
4.5.1. Syslog en sistemas Windows 4-2
4.6. CONFIGURACIÓN DE EDITRAN/PROXY WINDOWS Y UNIX 4-2
4.7. DIRECCIONES IP SIN TRAZA 4-4
4.8. DIAGNÓSTICOS DE LIBERACIÓN 4-4
4.9. ARRANQUE Y PARADA UNIX 4-5

1. INTRODUCCION Y REQUERIMIENTOS.

EDItran/Proxy, es una utilidad software que se implementa junto con EDItran/TCP, y sirve para dotar a éste último de mayor seguridad y control.

En el esquema siguiente, se presenta un diseño básico de conexiones IP en z/OS, con accesos controlados por 2 cortafuegos, normalmente de distinta tecnología. Sin embargo, en dicho esquema aparecen ñdos situaciones de funcionamiento distintoò (ambas con EDItran corriendo bajo TCP/IP en el monitor de teleproceso):

- Que todos los datos EDItran, incluso conexiones, tomen el camino ñnormalò, es decir, en ambos sentidos el camino sería: z/OS-Router-Firewall-Firewall-red IP-remoto . Esta sería la situación normal con EDItran/TCP.
- Que todos los datos EDItran, incluso conexiones, tomen en ambos sentidos el camino z/OS-Router-Firewall-**Proxy EDItran**-Firewall-red IP-remoto. Esta sería la situación con EDItran/TCP incluyendo EDItran/Proxy (software que corre en Proxy EDItran). Proxy EDItran es una máquina **Windows**, **UNIX** o **Linux** que está ubicada en la DMZ de la entidad.



En la primera situación, cuando se trabaja **sin EDItran/Proxy,** se plantean una serie de inconvenientes:

- **El host no está aislado del exterior. De alguna manera ñes visto directamenteò desde los extremos finales.**
- **Los firewall-router deben ser administrados constantemente. Cuando una entidad remota nos da su dirección IP, normalmente la deberemos habilitar. Cuando esa entidad cambia de IP, deberemos ñrefrescarlaò. Lo mismo ocurre con los puertos remotos (en caso de que se controlen). A su vez, cuando cambian las IP internas (z/os), requiere ñrefrescarò esos cambios. Toda esta situación de mantenimiento se complica con el uso generalizado de NAT.**

En la segunda situación, cuando se trabaja **con EDItran/Proxy,** se da solución a las incertidumbres anteriores:

- **El host queda aislado del exterior. Su única conexión y transmisión de datos posible queda relegada al intercambio en ambos sentidos de datos entre z/OS-router-firewall-Proxy EDItran. Para que esos datos lleguen a la entidad remota o sean recibidos desde la entidad remota, se habilita una segunda vía Servidor-proxy-firewall-red IP-remoto. No se trata de una doble transmisión de datos, como se explicará después.**
- Los mantenimientos y administración de router-firewall, son mínimos. A los extremos finales se les proporciona la IP y puerto de escucha del Proxy EDItran, de forma que sólo conocen dicha IP. Esto permite ñhabilitarò la totalidad de la red externa para que sólo se acceda al proxy. El EDItran/Proxy, sólo habilitará una conexión con el host cuando esté seguro de que en el extremo final dialoga un EDItran.

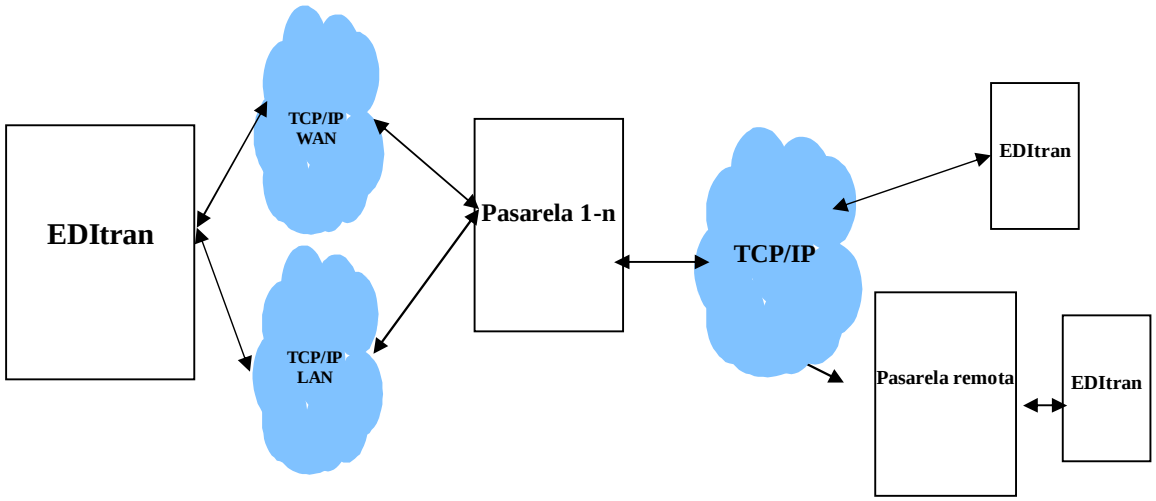
Las características y elementos del EDItran trabajando con EDItran/Proxy son los siguientes:

- **EDItran/Proxy es un software que corre en la DMZ, en concreto en Proxy EDItran (además hay un software que corre también en el monitor de teleproceso). No se trata de un segundo EDItran intermedio. Se trata de un software que actúa como controlador y como pasarela de datos.**
- **EDItran/Proxy, requiere EDItran/TCP en el host. Se contrata de forma independiente a éste último y es en definitiva un software-hardware que añade seguridad a las transmisiones EDItran. En este sentido, en caso de que a EDItran/Proxy le llegue una llamada externa (extremo remoto EDI ó no EDI), le deben llegar además unos datos de usuario EDItran con formato reconocido. SI no le llegan ó no los reconoce, EDItran/Proxy cierra el socket que le abrieron desde el exterior, sin que el EDItran del monitor de teleproceso se ñpercate ni resienta de nadaò.**
- **Las características de la transmisión con EDItran/Proxy son:**
  - El host z/OS (también OS/390), dialoga a través de TCP/IP con software EDItran/Proxy, que corre en máquinas WINDOWS (NT, 2000,..), UNIX. (SOLARIS, AIX, HP) y Linux.
  - EDItran/Proxy dialoga con los extremos finales en **una conexión distinta a la anterior, pero en la misma transmisión de datos (no en una segunda transmisión).**
  - En llamadas salientes desde el monitor de teleproceso, éste, proporciona a EDItran/Proxy, la información TCP/IP necesaria para que se conecte al extremo remoto (dirección IP y puerto destino). EDItran/Proxy, mantiene abierto el socket del host y conecta un segundo socket con el extremo remoto. Desde ese momento, pasa a encaminar los datos de un socket a otro.
  - En llamadas entrantes al monitor de teleproceso, los extremos finales llaman a la dirección IP y puerto habilitados en EDItran/Proxy (a través de un socket), le envían

unos datos de usuario EDItran. Si EDItran/Proxy reconoce el formato de los mismos, abre un segundo socket con el monitor de teleproceso (dirección IP y puerto del z/OS), le pasa los datos de usuario y la información de la IP y puerto remoto. Desde ese momento, pasa a encaminar los datos de un socket a otro.

  - EDItran/Proxy si detecta errores TCP/IP, le proporciona los elementos de diagnóstico (errno y retcode) al monitor de teleproceso para informarle.

- **Utilizando EDItran/TCP + EDItran/Proxy en local, los extremos remotos pueden tener cualquiera de las siguientes configuraciones:**
  - EDItran/TCP
  - EDItran/TCP + EDItran/Proxy
- **Pueden existir hasta 3 EDItran/Proxy en la DMZ; para ello se indicará en EDItran/P del z/OS hasta 3 direcciones IP del servidor Proxy. De esta forma se consigue que se pueda hacer backup en caso de llamada saliente (por ejemplo si alguno de los servidores Proxy está caído), ó balanceo de carga, indicando a un grupo 1 de remotos que llamen al servidor Proxy 1, a un grupo 2 que llamen al servidor Proxy 2 y a un grupo 3 que llamen al Proxy 3. En esta situación se notificará a los grupos para que coloquen en distinto orden las IP de los distintos Proxy, por ejemplo, al grupo 3 se le dará la IP del servidor Proxy 2 para que la coloque en segunda posición y la IP del servidor proxy 1 para que la coloque en tercera posición, y así haga backup llamando a Proxy 2 en caso de que Proxy 3 esté caído ó por Proxy 1 en caso de que Proxy 2 y 3 estén caídos. (Sólo en CICS)**
- **EDItran puede funcionar simultáneamente con varios tipos de conexión (X25, TCP/IP, TX y Proxy, es decir puede tener simultáneamente una sesiones conectadas por X25, otras por LU 6.2, otras contra PAD privados, otras contra PAD públicos, otras contra TCP/IP nativo, otras por TCP contra remotos X25 y otras contra TCP/IP a través de un proxy.**
- **Requiere versión EDItran/P remota > 4.0 (ambos extremos deben tener al menos EDItran 4.1).**



2. DEFINICIONES Y CAMBIOS (OS/390 ï Z/OS).

2.1. Versión CICS

2.1.1. DEFINICIONES.

Para realizar las definiciones, consulte el manual IP41USIC (cics), excepto:

Definición del fichero EZACONFG. Al definir el listener, se especificará SECEXIT = EDITR-PR, de forma que se sepa que este listener va a atender a este tipo de conexiones. Si se dispone de EDItran/TCP, se definirá otro listener (asociado a otro puerto y otra transid con el mismo programa), con SECEXIT = EDITRAN

```
EZAC,ALTER,LISTENER
 APPLID       ===> BMCIDATR            APPLID of CICS System
 TRANID       ===> ZTBA                Transaction Name of Listener
 PORT         ===> 07777               Port Number of Listener
 IMMEDIATE    ===> NO                  Immediate Startup   Yes|No
 BACKLOG      ===> 020                 Backlog Value for Listener
 NUMSOCK      ===> 100                 Number of Sockets in Listener
 MINMSGL      ===> 004                 Minimum Message Length
 ACCTIME      ===> 060                 Timeout Value for ACCEPT
 GIVTIME      ===> 010                 Timeout Value for GIVESOCKET
 REATIME      ===> 000                 Timeout Value for READ
 FASTRD (*)   ===> YES                 Read Immediately    Yes|No
 TRANTRN      ===> NO                  Translate TRNID     Yes|No
 TRANUSR      ===> NO                  Translate User Data Yes|No
 SECEXIT      ===> EDITR-PR            Name of Security Exit
```

(*) FASTRD DESAPARECE EN VERSIONES ALTAS DE ZOS

En CICS, ADEMAS de todos los programas EDItran/TCP/IP, deben darse de alta los programas ZTBPO203 y ZTBPOTPR.

```
DEFINE PROGRAM(ZTBPO203) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
DEFINE PROGRAM(ZTBPOTPR) GROUP(EDITRAN) LANGUAGE(COBOL) DATALOCATION(ANY)
```

2.1.2. CAMBIOS EN EDItran/P.

CAMPOS NUEVOS EDItran/P (PERFILES).

Para ver las definiciones, consulte el manual ED41USUC capítulo 1.3.1 (cics). Vea las pantallas de entorno local (segunda pantalla) y sesión (primera pantalla).

En el registro de entorno local, se definen:

- **Las direcciones IP (hasta 3) de el / los proxys locales. Sirven para 2 cosas:**
  - En caso de llamada saliente, el CICS establece una conexión con dicho proxy local y le acaba pasando la ip destino. Se hacen backup de proxy local de la misma forma que se haría con x25. Por ejemplo, si hay más de 1 y está caído, se asegura así que la conectividad con el remoto se hará con el segundo ó el tercero.
  - En caso de llamada entrante, se valida la dirección ip del proxy que nos pasa la llamada, si así se especifica en el registro de sesión

- **API TCP.**
- **TCPNAME.**
- **TIME-OUT USER DATA MAX(MSS):**
- **NRO.CONEX.SIMULT.LISTENER: .**

En cuanto **al registro de sesión**, se definirá lo siguiente:

- **TIPO DE CONEXION (Y = EDItran/PR, siempre en el extremo local). Si el remoto no tiene proxy, en su perfil el tipo de conexión será I (TCP/P). Si el remoto tiene a su vez un proxy, ambos extremos codifican Y.**
- **LINEAS REMOTAS TCP/IP. Dirección ip y puerto de la máquina REMOTA (no la del proxy).**
- **TC. No es obligatorio. Si se pone (sólo sirve cuando vers-editran-remota < 4.1), deben codificarse tantos como direcciones proxy en entorno local.**

CONSULTA DE LA TRAZA.

Se ha implementado un protocolo de mensajes de red que es fácilmente interpretable por su similitud a X25, con solicitud de llamada X0B, aceptación X0F y liberación X13 El socket es el número de tarea CICS y la lu es el puerto local ó remoto (dependiendo de si es llamada entrante ó saliente). Se incluye un mensaje x20 para visualizar errores (consulte el log con causa-diagnóstico. La documentación sobre ERRNO, RETCODE y mensajes de error en la TCPCICS, proporcionados por las macros utilizadas para SOCKET EXTENDIDOS se encuentra disponible en el apéndice C del manual IBM TCP/IP for MVS. CICS TCP/IP Socket Interface Guide and Reference. Document Number SC31-7131-03. Program number 5655 HAL. File Number S370/4300/30xx-50. Ver también Document Number: SC31-8518-00. Si no aparece el errno correspondiente puede que el error se trate de OS390 V2R5 OPEN EDITION, de modo que venga en F1AF9000 IP Planning and Migration Guide

```
    16/06/2004              CONSULTA DE FICHEROS               EDITRAN 4.1
    08:33:02                 CONSULTA DE TRAZA

    SESION :                                              FECHA :  16/06/2004
SEL           SESION               HORA  S MSJE NSM/LU T        COMENTARIO
 = ============================ ====== = ==== ====== = ==================
   S00DI S00TI EDIPR1            083230 S STC           T/O DE CONEXION
   S00DI S00TI EDIPR1            083230 S ETT  07777      0B      0002
   S00DI S00TI EDIPR1            083233 E ETT  07777      0F 00D8 0002
   S00DI S00TI EDIPR1            083233 S SAP           PET. NOTIFICACION  00
   S00DI S00TI EDIPR1            083233 S STN           T/O DE NOTIFICACION
   S00DI S00TI EDIPR1            083237 E SAR+          RESP. NOTIFICACION 00
   S00DI S00TI EDIPR1            083249 E E11           PETICION LIBERACION
   S00DI S00TI EDIPR1            083249 S SAB           SOL.  LIBERACION   02
   S00DI S00TI EDIPR1            083249 E ETT  07777      13 00D8 0000 00 0F
 S S00DI S00TI EDIPR1            083258 E ETT  03827      0B 00FD
   S00DI S00TI EDIPR1            083258 S ETT  03827      0F 00FD
   S00DI S00TI EDIPR1            083258 S STS           T/O DE ESPERA DE SAP
   S00DI S00TI EDIPR1            083302 E SAP           IND. NOTIFICACION  00
   S00DI S00TI EDIPR1            083302 S SAR+          RESP. NOTIFICACION 00
```

El significado de la traza previa es el siguiente, por ejemplo para el mensaje marcado:

1. En las columnas S y Comentario aparece un mensaje entrante (E) y se trata de un mensaje x0Bô (indicación de llamada).
2. En la columna NSM/LU aparece el puerto remoto (3827).
3. En la columna Comentario aparece un cvc , x00FDôó 253 en decimal, que es en realidad el número de tarea CICS (transid ZTBB) que trata la indicación de conexión. Es importante resaltar que si en un tiempo muy corto dicho número va pegando saltos muy grandes, nos encontraremos

con que el CICS se encuentra muy cargado (está ejecutando muchas tareas simultáneamente). Si se detectan problemas en el CICS, revise el entorno local (nro conexiones por listener), la parametrización de la definición CICS a VTAM, en concreto el parámetro EAS (número de comunicaciones activas simultáneamente) y la relación de os parámetros Tclass de las transacciones con el parámetro CMXT de la SIT (las transid se pueden apuntar a una clase, y en la SIT se limita en número de transid de cada una de las clases. En la SIT está el parámetro MXT para indicar el número de transid CICS.

4. En algunos casos, aparecen unos dígitos, que se corresponden con el CNID (identificador de aplicación, en caso de solicitud de llamada, para que devuelva lo mismo en llamada aceptada.
5. Otros tipos de mensaje son x'0F' (llamada aceptada), x'13' (liberación) y x'20' (error), además del propio x'0B' que si tiene sentido S significa solicitud de llamada.
6. En caso de EDItran/Proxy la clave de mensaje es ETT.

Si seleccionamos el mensaje anterior (traza expandida), vemos el contenido completo de la llamada entrante (entre otras cosas aparecen los campos anteriormente descritos x'0B'):

x'C5E3E340' es la clave de ETT ó
X'0B' indica sol-lla.
X'0EF3' es el puerto EDItran/PROXY de windows-unix (3827).
X'00FD' es el identificador del número de tarea (253).
X'E8' Indica el tipo de conexión (Y).
X'0F' es la longitud de datos de usuario (15)
X'C0....0A' son los datos de usuario x25.
X'F1F7....F6' es la ip de EDItran/PROXY de windows-unix (172.022.164.076)
X'1E69' es el puerto remoto (7779)
X'D6E2F3F0F0C2', en ebcdic OS390B es el DNS asociado a la ip final (remoto).

```
16/06/2004              CONSULTA DE FICHEROS                EDITRAN 4.1
  08:43:19                 CONSULTA DE TRAZA

            SESION TRAZA...: S00DI S00TI EDIPR1

FECHA SSAAMMDD.: 20040616    HORA HHMMSS....: 083258    ENTRADA/SALIDA.: E

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....
C5E3E3400B00000EF300FD00000000000000000000D700000000000000000000FC0A3300000
999304544495458310A00000000000000000000000000000000000000000000000404040
4040404040404040404040404040404040404040404040404040404040404040404040404040
4040404040404040F1F7F24BF0F2F24BF1F6F44BF0F7F61E6340404040404040404040404040
4040404040404040404040404040404040404040404040404040404040404040404040404040
4040404040404040D6E2F3F9F0C2F1F0F0F0F9F9F9F4F0F2F0F0F0F9F9F9F4F0C5C4C9
D7D9F1000000000000000000000000000000000000000000000000000000000000000000000
01B3404040000404040F0F8F3F2F5F8404040404040

       PF2: SWITCH HEXADECIMAL - CARACTER
```

Si pulsamos PF2, se visualiza en mensaje en formato texto y además se incluye información sobre la hora real de proceso (no tiene porqué ser la misma que la de la traza) y sobre la longitud del mensaje tratado (no tiene porqué ser el mismo que el que está en red).

```
16/06/2004              CONSULTA DE FICHEROS                EDITRAN 4.1
  08:53:06                CONSULTA DE TRAZA
            SESION TRAZA...: S00DI S00TI EDIPR1

FECHA SSAAMMDD.: 20040616    HORA HHMMSS....: 083258    ENTRADA/SALIDA.: E

....+....1....+....2....+....3....+....4....+....5....+....6....+....7....
ETT .  .3 .          P         .{t.  rr........
                                          172.022.164.076.   ...c..
                                           OS390B10009994020009994 0EDI
PR1
                                    ..        083258

HORA DE PROCESO DE MENSAJE : 083258
LONGITUD DE MENSAJE TRATADO: 000435

       PF2: SWITCH HEXADECIMAL - CARACTER
```

Para trazas de más detalle de INDRA, codificar sistema-operativo = EDPR, versión-sistema-operativo = spaces ó MULT, y Número-cvcs-máximos = 999. En este caso, se crean cola ts ZTBPEDPR (MULT) ó colas TS ZTBH+(MMSS , minutos, segundos) (spaces), con datos sobre escrituras y lecturas de la red, a ser analizados por INDRA.

2.1.3. BACKUP.

El sistema de backup, en caso de que falle una llamada es el siguiente:
Dir-ip-proxy-local (1) ï Dir-ip-remota (1)
Dir-ip-proxy-local (1) ï Dir.ip.remota (2)
Dir-ip-proxy-local (1) ï Dir.ip.remota (3)
Dir-ip-proxy-local (2) ï Dir-ip-remota (1)
Dir-ip-proxy-local (2) ï Dir.ip.remota (2)
Dir-ip-proxy-local (2) ï Dir.ip.remota (3)
Dir-ip-proxy-local (3) ï Dir-ip-remota (1)
Dir-ip-proxy-local (3) ï Dir.ip.remota (2)
Dir-ip-proxy-local (3) ï Dir.ip.remota (3)

2.1.4. Mensajes de error xô20ô y liberación xô13ô

Consulte el manual IP41USIC. (cics)

2.2. Versión IMS

Se requiere la misma instalación que para EDItran/TCP. Para ver las definiciones, consulte el manual IP41USII

Los parámetros afectados de los perfiles de EDItran/P se enumeran en el citado manual y están descritos en el manual de usuario de EDItran/P, consulte el manual EP41USUI.

En la consulta de la traza se han introducido nuevos mensajes que permiten identificar las sesiones que utilizan el proxy, pero que son análogos a los mensajes que aparecen cuando se utiliza TCP nativo.

```
 31/01/05                    CONSULTA DE LA TRAZA                    EDITRAN
 09:13:00                                                              4.1

         SESION           FECHA   HORA    S CLA C  NSM            COMENTARIO
------------------------ ----- -------- - --- - ------ ------------------------
00009993000000010PRUEBA 31-01 09:12:05 S E00          PETICION DE CONEXION
00009993000000010PRUEBA 31-01 09:12:07 E E00          PETICION DE CONEXION
00009993000000010PRUEBA 31-01 09:12:07 S X00          INDICACION CONEXION
00009993000000010PRUEBA 31-01 09:12:08 E X00          INDICACION CONEXION
00009993000000010PRUEBA 31-01 09:12:29 E SAB          LIBERACION POR OPERADOR
00009993000000010PRUEBA 31-01 09:12:29 S E11          PETICION LIBERACION
00009993000000010PRUEBA 31-01 09:12:31 E E11          PETICION LIBERACION
00009993000000010PRUEBA 31-01 09:12:31 S X11          INDICACION LIBERACION
00009993000000010PRUEBA 31-01 09:12:31 S CLO        0 CIERRA CONEXION TCP
00009993000000010PRUEBA 31-01 09:12:32 E X11          INDICACION LIBERACION
00000000000000000000000 31-01 09:12:33 E CON        1 INDICACION CONEXION TCP
00009993000000010000001 31-01 09:12:33 E TAK        0 ACEPTA CONEX. TCP(PROXY)
00009993000000010000001 31-01 09:12:33 S X00          INDICACION CONEXION
00009993000000010000001 31-01 09:12:34 E X00          INDICACION CONEXION
00009993000000010000001 31-01 09:12:34 E SAP          PETICION SESION REMOTA
00009993000000010000001 31-01 09:12:34 S SAR          ACEPTACION PET. SESION


 31/01/05                    CONSULTA DE LA TRAZA                    EDITRAN
 09:20:33                                                              4.1

         SESION           FECHA   HORA    S CLA C  NSM            COMENTARIO
------------------------ ----- -------- - --- - ------ ------------------------
00009993000000010PRUEBA 31-01 09:19:09 S X11          INDICACION LIBERACION
00009993000000010PRUEBA 31-01 09:19:13 E X11          INDICACION LIBERACION
00009993000000010PRUEBA 31-01 09:19:56 E E00          PETICION DE CONEXION
00009993000000010PRUEBA 31-01 09:19:56 S SOC        0 PETICION CONEXION TCP
00009993000000010PRUEBA 31-01 09:19:56 S CON        0 PETICION CONEXION TCP
00009993000000010PRUEBA 31-01 09:19:57 S X00          INDICACION CONEXION
00009993000000010000001 31-01 09:19:57 E E00          PETICION DE CONEXION
00009993000000010000001 31-01 09:19:57 S SOC        1 PETICION CONEXION TCP
00009993000000010000001 31-01 09:19:57 S CON        1 PET. CONEXION TCP(PROXY)
00009993000000010000001 31-01 09:19:57 S X00          INDICACION CONEXION
00009993000000010PRUEBA 31-01 09:20:17 E X00          INDICACION CONEXION
00009993000000010PRUEBA 31-01 09:20:18 S SAP          PETICION SESION
00009993000000010000001 31-01 09:20:18 E X00          INDICACION CONEXION
00009993000000010000001 31-01 09:20:18 S SAP          PETICION SESION
00009993000000010PRUEBA 31-01 09:20:22 E SAR          ACEPTACION PET. SESION
00009993000000010000001 31-01 09:20:22 E SAR          ACEPTACION PET. SESION
```

En cuanto a la consulta de la traza expandida se ha modificado lo que se muestra en pantalla para los mensajes de TCP, a continuación se incluyen unos ejemplos.

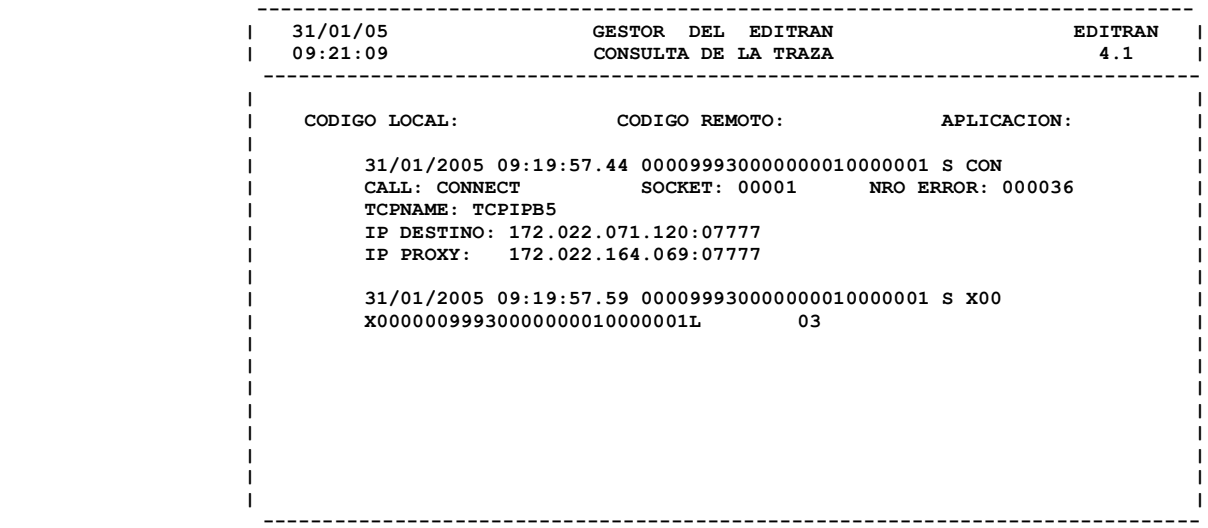
Mensaje entrante para sesión con proxy

```
 ------------------------------------------------------------------------------
|   31/01/05                GESTOR  DEL  EDITRAN                    EDITRAN   |
|   09:12:40                CONSULTA DE LA TRAZA                      4.1     |
 ------------------------------------------------------------------------------
|                                                                              |
|    CODIGO LOCAL:             CODIGO REMOTO:             APLICACION:          |
|                                                                              |
|         31/01/2005 09:12:33.53 00000000000000000000000 E CON                 |
|         MENSAJE CONEXION       SOCKET: 00001      NRO ERROR:                 |
|         LISTENER: KI0E8A2L     PUERTO: 07777                                 |
|         IP REMOTA:  172.022.164.069                                          |
|                                                                              |
|                                                                              |
|         31/01/2005 09:12:33.53 00009993000000010000001 E TAK                 |
|         CALL: TAKESOCKET       SOCKET: 00000      NRO ERROR: 000000          |
|         TCPNAME: TCPIPB5                                                     |
|         IP ORIGEN:  172.022.071.120                                          |
|         IP PROXY:   172.022.164.069                                          |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
 ------------------------------------------------------------------------------
```

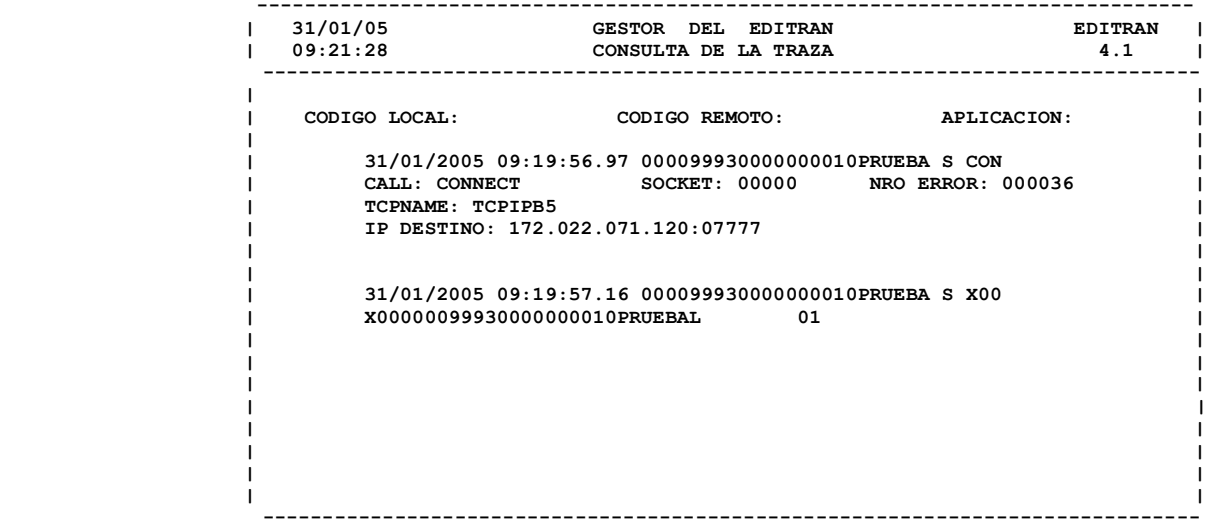
Mensaje entrante para sesión sin proxy

```
 ------------------------------------------------------------------------------
|   31/01/05                GESTOR  DEL  EDITRAN                    EDITRAN   |
|   09:11:16                CONSULTA DE LA TRAZA                      4.1     |
 ------------------------------------------------------------------------------
|                                                                              |
|    CODIGO LOCAL:             CODIGO REMOTO:             APLICACION:          |
|                                                                              |
|         31/01/2005 09:10:59.35 00000000000000000000000 E CON                 |
|         MENSAJE CONEXION       SOCKET: 00001      NRO ERROR:                 |
|         LISTENER: KI0E8A2L     PUERTO: 07777                                 |
|         IP REMOTA:  172.022.071.120                                          |
|                                                                              |
|                                                                              |
|         31/01/2005 09:10:59.35 0000999300000000010PRUEBA E TAK               |
|         CALL: TAKESOCKET       SOCKET: 00000      NRO ERROR: 000000          |
|         TCPNAME: TCPIPB5                                                     |
|         IP ORIGEN:  172.022.071.120                                          |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
|                                                                              |
 ------------------------------------------------------------------------------
```

Mensaje saliente para sesión con proxy



Mensaje saliente para sesión sin proxy


31/01/05 GESTOR DEL EDITRAN EDITRAN
09:21:28 CONSULTA DE LA TRAZA 4.1
CODIGO LOCAL: CODIGO REMOTO: APLICACION:
31/01/2005 09:19:56.97 0000999300000000010PRUEBA S CON
CALL: CONNECT SOCKET: 00000 NRO ERROR: 000036
TCPNAME: TCPIPB5
IP DESTINO: 172.022.071.120:07777
31/01/2005 09:19:57.16 0000999300000000010PRUEBA S X00
X00000099930000000010PRUEBAL 01

3. Características principales

La implantación cada vez más amplia del protocolo TCP/IP en EDItran viene asociada a nuevas necesidades que surgen a raíz de la utilización de Internet. Internet aporta un gran número de ventajas a la comunicación entre extremos, pero también añade una serie de incertidumbres como por ejemplo es el tema de seguridad de las comunicaciones.

Aquí surge la necesidad de utilizar productos como *firewalls* que nos permitan controlar en lo posible las incertidumbres de seguridad y de otros productos como EDItran/PX específicamente desarrollado para EDItran y que evitará la mayoría de los ataques de *DoS* (Denegación de Servicio), *bombing*, ... mintiendo así el *HOST* de los posibles peligros de situarlo en la zona desmilitarizada.

A continuación se detallarán algunas de las características que hacer a EDItran/PX un elemento imprescindible en una red pública TCP/IP.

3.1. MultiPlataforma

EDItran/PX está disponible para los sistemas operativos Windows de Microsoft y para sistemas operativos UNIX, como Solaris, Linux...

Permitiendo, de ésta manera elegir la plataforma adecuada a cada necesidad.

3.2. Optimización (MultiThreading)

Uno de los principales preocupaciones a la hora de diseñar EDItran/PX ha sido la búsqueda de la mayor eficiencia posible. De ésta manera EDItran/PX está construido de manera que crea un hilo de ejecución por cada cliente conectado, permitiendo tanto que una conexión no afecte a las demás como que se consiga la máxima eficiencia en sistemas multi-procesador.

3.3. TimeOut

Existe un *TimeOut* independiente y previo a la conexión con EDItran en el HOST que cerrará la conexión a un cliente cuando éste se conecte pero no envíe ningún dato. De ésta manera se evita que el HOST pueda ser atacado mediante un intento de *DoS* por falta de conexiones libres.

3.4. Bombing

Además de contar con un *TimeOut*, EDItran/PX cuenta con un sistema que evita el intento de conexiones múltiples desde un mismo cliente con ánimo de intentar un *Dos*. Estas conexiónes no llegarán nunca al EDItran interno evitando cargarlo y además cuando se detecta un intento de bombing se deconecta la conexión con el causante.

3.5. Seguridad

Cómo ya se ha mencionado, EDItranPX evita tener que colocar EDItran en la zona desmilitarizada o DMZ ya que allí es donde irá EDItran/PX. De manera que se aumenta la seguridad ya que EDItran se mantiene en la red interna, fuera de la DMZ.

3.6. Validación de protocolo EDItran

Una de las caráterísticas principales de EDItran/PX es que *conoce* el protocolo de EDItran y de ésta manera evitará que lleguen al EDItran interno conexiones que no cumplan el protocolo, haciendo de ésta manera un trabajo previo y liberando a EDItran del mismo.

3.7. Generación de Syslog

EDItran/PX dispone de un sistema de generación de log propio y también utiliza el syslog del sistema que permite almacenarlo o enviar el mismo log a otra máquina.

Para más detalles consultar el apartado 4.5.

4. EDItran/Proxy EN UNIX Y WINDOWS

Los elementos necesarios para el correcto funcionamiento del sistema EDItran/Proxy en los entornos UNIX-WINDOWS son:

- Protocolo TCP/IP instalado.
- Software EDItran/Proxy instalado y con licencia de uso.

4.1. Instalación de EDItran/Proxy en UNIX

En los entornos UNIX el Software EDItran/Proxy se distribuye como un fichero tar comprimido con GNU Zip.

Por ejemplo, si se ha recibido el fichero ediproxy.sparc-sun-solaris.tar.gz deberá ejecutar lo siguiente:

gunzip ediproxy.sparc-sun-solaris.tar.gz
tar ï xf ediproxy.sparc-sun-solaris.tar

4.2. Instalación de EDItran/Proxy en WINDOWS

En Windows se proporciona un programa de instalación. Para llevar a cabo la instalación se debe seleccionar el botón de INICIO y al desplegarse el menú elegir la opción Ejecutar.

Si la unidad donde se encuentra el producto para instalar fuera ñE:ò, teclee lo siguiente:

E:\EDItranProxy.exe

Siga las instrucciones que vayan apareciendo por la pantalla. Si se decide crear un servicio para el control del EDItranProxy tendrá las siguientes características.

4.3. Configuración de EDItran/Proxy WINDOWS

En el mismo proceso de instalación se deben indicar las direcciones IP y puertos locales de escucha, así como la dirección IP del HOST y puerto de escucha del mismo, aunque en cualquier momento se puede consultar la configuración o modificarla utilizando el comando *confproxy* (ver sección 4.6).

4.4. Arranque y parada WINDOWS

Si durante el proceso de instalación se ha elegido la opción de crear un servicio, el arranque se deberá hacer desde el mismo ñServicio Proxy de EDItranò teniendo los permisos necesarios, si no se eligió instalar / crear el servicio, se podría arrancar desde una ventana de interfaz de comando (cmd) ejecutando el fichero ñediproxyth.exeò

4.5. Notificaciones syslog

En los sistemas UNIX existe una manera estándar y muy utilizada de enviar y mantener almacenar mensajes de log, ese sistema se conoce como syslog. En los sistemas UNIX existe un demonio *syslogd* que recibe las peticiones UDP en el puerto 514 de log y lo transfiero o almacena dependiendo de la configuración.

EDItranPX genera una salida por cada conexión y desconexión que se realiza a través de él, además también genera información de arranques, paradas. Además, para permitir, de una forma sencilla, controlar esa sálida va redirigida a log del sistema o syslog. Los mensajes que se envían con un nivel de error *LOG_NOTICE*. Para poder administrar donde se reciben esos mensajes hay que editar el fichero */etc/syslog.conf*.

4.5.1. Syslog en sistemas Windows

El sistema operativo Windows no posee la funcionalidad de syslog, sin embargo existe mucho software creado para poder recoger y almacenar la salida que se pueda generar hacia el syslog (por ejemplo la compañía *haneWin* dispone de un servidor gratuito de syslog en http://www.hanewin.net/syslog-e.htm o bien la compañía *Kiwi Enterprises* dispone del producto *Kiwi Syslog Daemon* también gratuíto en http://www.kiwisyslog.com/syslog-info.php).

Desde un sistema Windows podremos decidir enviar el syslog a un sistema UNIX o bien a un servidor syslog Windows, para ello hay que editar o crear el fichero syslog.cfg en el mismo directorio donde se encuentra instalado EDItranPX y escribir la dirección IP de la máquina destino del syslog.

Si se desea obtener esta información en un fichero se arrancará EDItran/Proxy como proceso y se ejecutará el comando

ediproxyth 2> "nombre de fichero de log"

4.6. Configuración de EDItran/Proxy Windows y UNIX

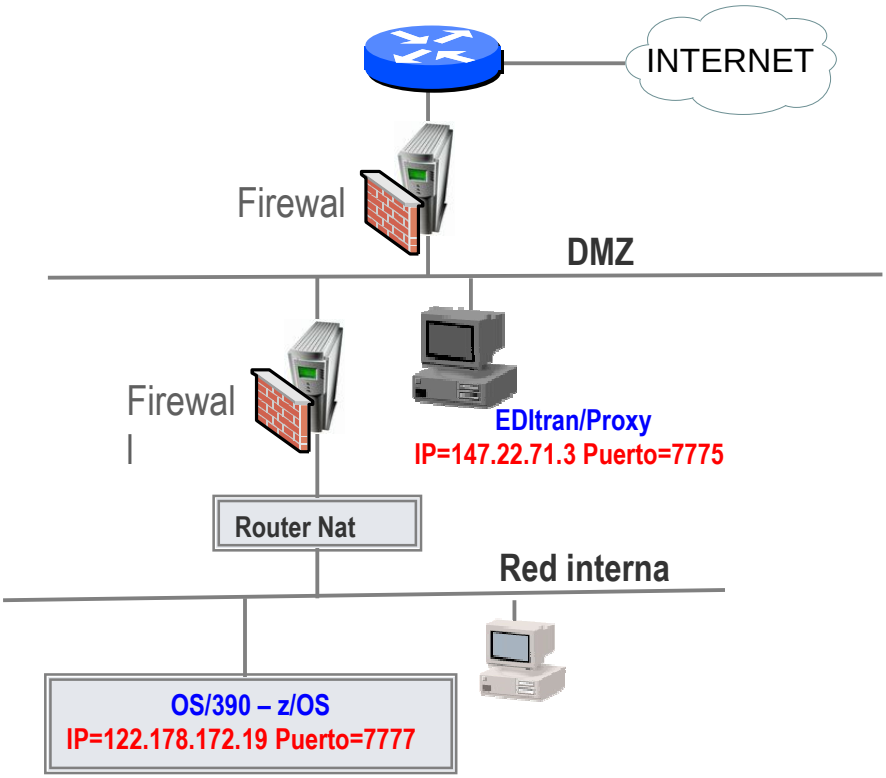
Una vez instalado es necesario establecer algunos parámetros necesarios para el funcionamiento del EDItran/Proxy. Para ello se proporciona el siguiente comando que hay que ejecutar antes de arrancar el sistema por primera vez.

```
confproxy V4.1 R4 - Aug 26 2004
Copyright (C) 1991-2004 INDRA
No hay entorno local definido
Forma de uso:
confproxy <ip host> <puerto host> <ip local> <puerto local> [ip Permitida 1]
[ip
 Permitida 2] ... [ip Permitida n]
donde:
        <ip host>:         (Obligatorio) Direccion IP del Host.
        <puerto host>:     (Obligatorio) Puerto del Host.
        <ip local>:        (Obligatorio) Direccion IP Local de escucha.
        <puerto local>:    (Obligatorio) Puerto de escucha local.
        [ip Permitida n]: (Opcional) Ips permitidas.
```

Ejemplo:

Con una red con las direcciones que se muestran en el siguiente gráfico, los parámetros ña pasarò al comando confproxy seria:

confproxy 122.178.172.19 7777 147.22.71.3 7775



Si se ejecuta el comando si ningún parámetro veremos la configuración actual.

```
confproxy V4.1 R4 - Aug 26 2004
Copyright (C) 1991-2004 INDRA

Configuracion actual del entorno local:
Nombre (o IP) - puerto del HOST  : 122.178.172.19 - 7777
Nombre (o IP) - puerto de escucha: 147.22.71.3 - 7775
Existen 0 IPs permitidas.

Forma de uso:
confproxy <ip host> <puerto host> <ip local> <puerto local> [ip Permitida 1]
[ip Permitida 2] ... [ip Permitida n]
donde:
        <ip host>:         (Obligatorio) Direccion IP del Host.
        <puerto host>:     (Obligatorio) Puerto del Host.
        <ip local>:        (Obligatorio) Direccion IP Local de escucha.
        <puerto local>:    (Obligatorio) Puerto de escucha local.
        [ip Permitida n]:  (Opcional) Ips permitidas.
```

Dentro de éste comando existe un parámetro opcional ñIps permitidasò que nos permiten limitar las direcciones desde las que se puede utilizar EDItran /Proxy en nuestra red.

4.7. Direcciones IP sin traza

Pueden existir dentro de una organización herramientas de monitorización de la red (como *HP Openview*, *Service Monitoring Daemon*, *LANsurveyor*, *ipMonitor*...). Estos sistemas intentan de forma periódica conectarse con un servicio en alguna máquina de red para comprobar si éste continua todavía activo y aceptando conexiones.

Para evitar que se llene el fichero *ediproxyth.out* de información que no deseamos sobre estos sistemas, existe la posibilidad de crear un fichero con una serie de direcciones TCP/IP de las que no deseamos que aparezca su actividad en la traza de EDItran/PX.

De esta manera, podemos incluir en un fichero todas las direcciones TCP/IP donde tengamos sistemas de monitorización y evitaremos llenar el fichero de *ediproxyth.out* de líneas carentes de información útil.

Las direcciones TCP/IP de las que no se desea traza se deben introducir cada una en una línea en el fichero ***ipnotraza.cfg*** en el directorio donde se encuentre instalado EDItran/PX. Puede no existir el fichero ***ipnotraza.cfg*** en este caso el fichero *ediproxyth.out* contendrá toda la información.

A continuación se muestra el contenido de un fichero *ipnotraza.cfg* que contiene dos Ips (172.22.168.23 y 172.22.168.24) de las que no se desea traza en el fichero *ediproxyth.out*::

172.22.168.23

172.22.168.24

4.8. Diagnósticos de Liberación

A continuación se muestran los códigos de liberación de EDItran/PX.

Código de Liberación	Descripción
1	Se ha producido un Time Out.
2	No se ha podido conectar con el EDItran remoto.
3	No se han podido enviar los Datos de Usuario al remoto
4	Error al enviar datos al remoto.
5	Se ha recibido un Close del remoto
6	Se ha recibido un Error del remoto
7	IP de origen no permitida.
8	Los datos de Usuario Encapsulados no son correctos
9	No son correctos los datos de Usuario
11	Se ha llegado al límite de conexiones simultaneas
12	La longitud de los Datos de Usuario es incorrecta
13	No se ha podido resolver el dns del remoto

4.9. Arranque y parada UNIX

Para arrancar y parar EDItran/Proxy ejecute EDIProxy start y EDIProxy stop.

ediproxy start ï h156.122.34.12:8888

En los entornos UNIX ediproxy es el script que se lista a continuación.

```
#!/bin/sh
#########################################################################
#       Direccion de Comunicaciones
#       (C) INDRA, S.A   Enero, 1999.
#
#     sh shell script de arranque/parada del sistema EDItranPX.
#
#########################################################################

#EDI_IPC_KEY_BASE=8000
#export EDI_IPC_KEY_BASE

##################
#SUN, DEC y LINUX
LD_LIBRARY_PATH=`pwd`:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH

##################
#AIX
LIBPATH=`pwd`
export LIBPATH

##################
#HP
SHLIB_PATH=`pwd`
export SHLIB_PATH
#export X25_IFNAME_A=NXL0
#export X25_IFNAME_B=NXL1
#export SNCE_DES_LIB=/$CICSREGION/lib
#export SNCE_PROGRAM_KEYS=/$CICSREGION/ftesbatch/NXEN2EDI

##################
#DEC DTE CLASS DEFINITION
#X25_DTE_CLASS_A=llc2-class-a
#export X25_DTE_CLASS_A
#X25_DTE_CLASS_B=llc2-class-b
#export X25_DTE_CLASS_B

##################
#SOCKS5 SERVER
#SOCKS5_SERVER=proxy.indra.es:1080
#export SOCKS5_SERVER

PROC_STAR="ediproxyth"
PROC_STOP="ediproxyth"
N=`tput rmso`
B=`tput smso`
if ps -ef > /dev/null 2>&1; then
        PS="ps -ef"
else
```

```
        PS="ps -x"
fi

# arranque del proceso dado
startproc() {
    if [ -f $1 ]; then
      echo '*** Arranque  ***' - $USER - `date` >>$1.out
      if [ ! -z "$traza" ] ; then
          EDI_DEBUG=$1.traza
      else
          EDI_DEBUG=
      fi
      export EDI_DEBUG
      $1 >> $1.out 2>&1 &
      sleep 8
        pid=`$PS |
             grep $! | grep $1 | grep -v grep |
             awk  '{print $2}'`

        if [ "$pid" != "" ] ; then
          echo "Proceso $1 arrancado."
          return 0
      else
          echo "Proceso $1 NO ARRANCADO."
          return 1
      fi
    fi
}

# parada del proceso dado
stopproc() {
        pid=`$PS |
             grep $1 | grep -v grep |
             awk  '{print $2}'`

        if [ "$pid" != "" ] ; then
          kill -2 $pid > /dev/null 2>&1
          if [ $? = 0 ] ; then
            echo "Proceso $1 detenido."
            return 0
          else
            echo "Proceso $1 NO DETENIDO."
            return 1
          fi
      else
          echo "Proceso $1 no encontrado."
      fi
      sleep 4
}

# estado del proceso dado
statusproc() {
        pid=`$PS |
             grep $1 | grep -v grep |
             awk  '{print $2}'`

        if [ "$pid" != "" ] ; then
                return 0
            else
                return 1
```

```
        fi
}

#################################
traza=
force=
while getopts tf opcion
do
    case $opcion in
    t) traza=1 ;;
    f) force=1 ;;
    \?) printf "Opcion invalida\n" ;;
    esac
done

shift `expr $OPTIND - 1`
case $1 in
    'start')
      echo "Arrancando sistema EDItran/PX..."
#     if [ -z "$force" ] ; then
#         statusproc ediproxyth
#         if [ $? = 0 ]; then
#               echo "${B}Hay otro sistema EDItran/PX arrancado${N}."
#               exit 1
#         fi
#     fi

      for PROCESO in $PROC_STAR;
      do
          startproc $PROCESO
      done;
      statusproc ediproxyth
      if [ $? = 0 ]; then
            echo "Sistema EDItran/PX arrancado."
            exit 0
      else
            echo "${B}Sistema EDItran/PX NO ARRANCADO${N}."
            exit 1
      fi
      ;;
    'stop')
      echo "Deteniendo sistema EDItran/PX..."
      for PROCESO in $PROC_STOP;
      do
          stopproc $PROCESO
      done;
#     statusproc editranp
#     if [ $? = 0 ]; then
#           echo "${B}Sistema EDItran/PX NO DETENIDO${N}."
#           exit 0
#     else
            echo "Sistema EDItran/PX detenido."
            exit 1
#     fi
      ;;
    'status')
      echo "Estado sistema EDItran/PX..."
      statusproc ediproxyth
      if [ $? = 0 ]; then
            echo "${B}Sistema EDItran/PX arrancado${N}."
```

```
            exit 0
      else
            echo "Sistema EDItran/PX detenido."
            exit 1
      fi
      exit 0
      ;;
    *)
       printf "Usage: %s [-t] [-f] start|stop|status\n" $0
       printf "\t-t\t Traza\n"
#       printf "\t-f\t Ignora otro EDItran/PX arrancado\n"
       printf "\tstart\t Arranca el sistema EDItran/PX\n"
       printf "\tstop\t Detiene el sistema EDItran/PX\n"
       printf "\tstatus\t Obtiene el estado del sistema EDItran/PX\n"
       exit 1
       ;;
esac
```

BARCELONA
Avda. Diagonal, 218, 3º
08018 BARCELONA

BILBAO
Henao, 4, 4ºA
48001 BILBAO

MADRID
Avda. de Bruselas 35 - Arroyo de la Vega - Alcobendas
28108 MADRID

SEVILLA
Avda. San Francisco Javier, 22, 6º
41018 SEVILLA

VALENCIA
Colón, 60
46004 VALENCIA